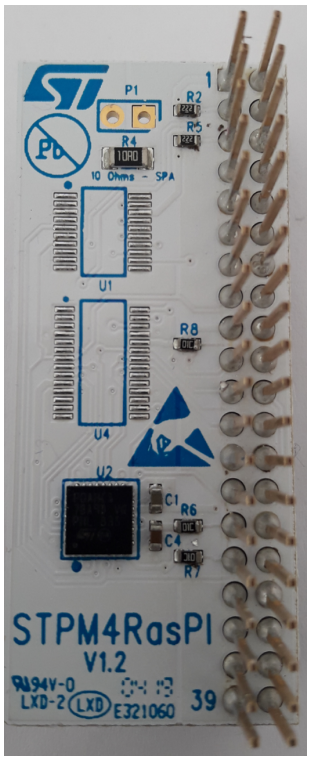
STPM4RasPI

Data brief

Raspberry Pi® extension board with an ST33 Trusted Platform Module



Product status link
STPM4RasPI

Features

- I²C TPM compatible serial interface
- SPI TPM compatible serial interface
- 40-pin female connector to plug on Raspberry Pi®
- 40-pin male connector to probe signal or connect another extension board
- P1 connector (optional) to measure the TPM power consumption
- Supported ST33 TPM devices:
  - ST33TPHF20SPI, ST33TPHF2ESPI, ST33TPHF2XI2C, ST33TPHF20I2C, ST33TPHF2EI2C and ST33TPHF2XSPI in VFQFPN32 package

Description

The STPM4RasPI is an official extension board to connect the ST33 TPM products to the Raspberry Pi® device. It is designed for development, proof of concept or demonstration activities. The board is shipped with one trusted platform module soldered (see ordering information for TPM product availability).

1 Main features

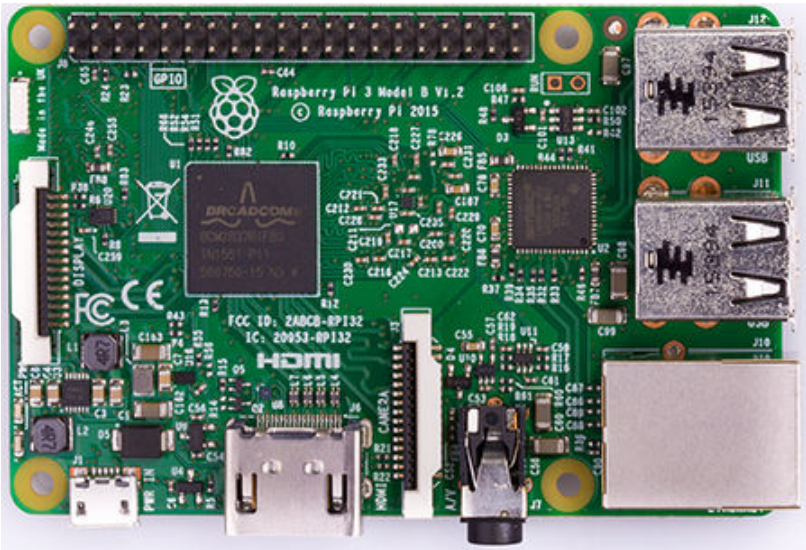
This section details the main features of STPM4RasPI, official extension board to connect the ST33 Arm®-based TPM products to the Raspberry Pi device.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.1 Raspberry Pi introduction

The Raspberry Pi 3 Model B is the third generation Raspberry Pi.

Figure 1. Raspberry Pi 3 Model B



The differences with the Raspberry Pi 2 are listed below:

- 1.2 GHz 64-bit quad-core ARMv8 CPU
- 802.11n wireless lan
- Bluetooth 4.1
- Bluetooth low energy (BLE)

The common features with the Raspberry Pi 2 are listed below:

- 1-Gbyte RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Ethernet port
- Combined 3.5 mm audio jack and composite video
- Camera interface (CSI)
- Display interface (DSI)
- microSD™ card slot (now push-pull rather than push-push)
- VideoCore® IV 3D graphics core

More details on this Raspberry Pi 3 are available on www.raspberry.org.

The STPM4RasPI is compatible with all Raspberry Pi versions supporting 40 GPIO pins.

1.2 Raspberry SPI/I²C connectivity by GPIO

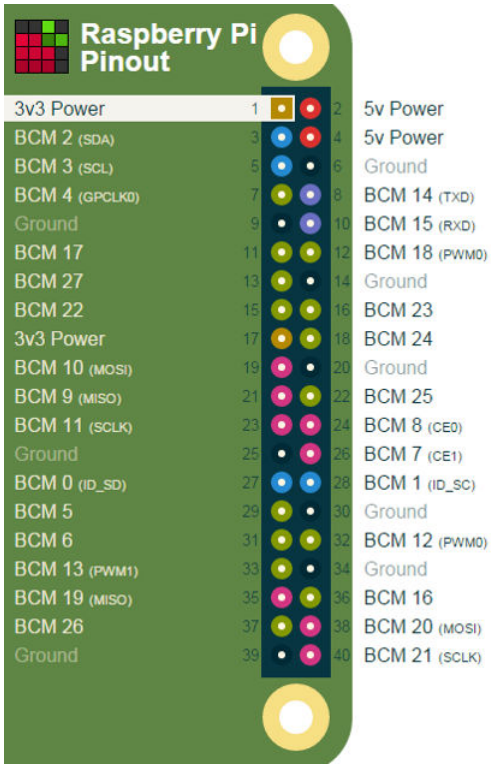
The ST33TPHF2ESPI, ST33TPHF2XSPI and ST33TPHF20SPI products use the following signals:

- MOSI (pin 19)
- MISO (pin 21)
- SCLK (pin 23)
- CE0 (pin 24)
- VCC (pin 17)
- GND (pin 25)
- RST (pin 18)
- PIRQ (pin 29)
- PP (pin 16)

The ST33TPHF2EI2C, ST33TPHF2XI2C and ST33TPHF20I2C products use the following signals:

- SDA (pin 3)
- SCL (pin 5)
- SCLK (pin 23)
- VCC (pin 1)
- GND (pin 6)
- RST (pin 18)
- PIRQ (pin 29)
- PP (pin 16)

Figure 2. Raspberry Pi GPIO



1.3 STPM4RasPI setup

The STPM4RasPI fits in perfectly in the standard Raspberry Pi box. The STPM4RasPI features a GPIO pin reserved for probing or connecting another extension board.

If the height size is critical for the system, and the GPIO is not needed, a specific STPM4RasPI exists without the GPIO (contact the local STMicroelectronics sales office).

Figure 3. STPM4RasPI embedded in the Raspberry Pi board

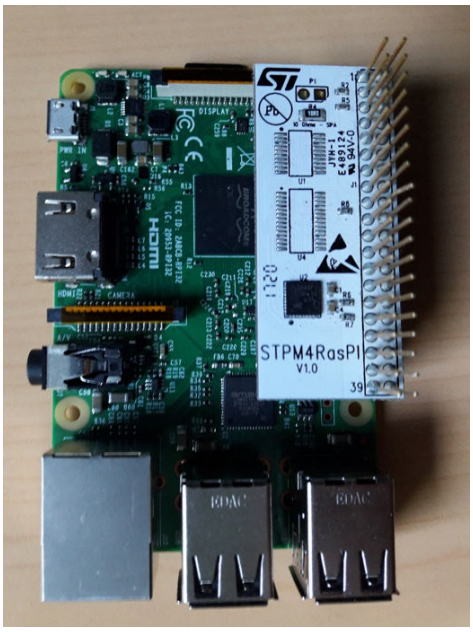


Figure 4. STPM4RasPI embedded in the Raspberry Pi box with touch screen

1.4 TPM power consumption

The P1 pin header can be soldered to plug a multimeter over a 10 Ω resistor (R4) in order to measure the TPM power consumption.

Figure 5. P1 header location

2 Linux® integration requirements

2.1 TPM Linux driver introduction

The TPM Linux SPI driver is included in the `Linux/drivers/char/tpm` directory:

https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/tree/drivers/char/tpm?h=v4.14.49

The ST33TPHF2ESPI, ST33TPHF2XSPI and ST33TPHF20SPI for SPI are TCG-compliant and support the following standard TCG Linux SPI drivers:

- *tpm_tis.c*
- *tpm_tis_spi.c*

Figure 6. TPM directory example in Linux kernel

Mode	Name
-rw-r--r--	Kconfig
-rw-r--r--	Makefile
d---------	st33zp24
-rw-r--r--	tpm-chip.c
-rw-r--r--	tpm-dev-common.c
-rw-r--r--	tpm-dev.c
-rw-r--r--	tpm-dev.h
-rw-r--r--	tpm-interface.c
-rw-r--r--	tpm-sysfs.c
-rw-r--r--	tpm.h
-rw-r--r--	tpm1_eventlog.c
-rw-r--r--	tpm2-cmd.c
-rw-r--r--	tpm2-space.c
-rw-r--r--	tpm2_eventlog.c
-rw-r--r--	tpm_acpi.c
-rw-r--r--	tpm_crb.c
-rw-r--r--	tpm_eventlog.h
-rw-r--r--	tpm_nsc.c
-rw-r--r--	tpm_of.c
-rw-r--r--	tpm_ppi.c
-rw-r--r--	tpm_tis.c
-rw-r--r--	tpm_tis_core.c
-rw-r--r--	tpm_tis_core.h
-rw-r--r--	tpm_tis_spi.c
-rw-r--r--	tpm_vtpm_proxy.c
-rw-r--r--	tpmrm-dev.c
-rw-r--r--	xen-tpmfront.c

The TCG TPM driver is functional from Linux kernel 4.8. In the configuration specification, check if all labels listed below are inserted:

- CONFIG_TCG_TPM = y
- CONFIG_TCG_TIS_CORE = y
- CONFIG_TCG_TIS_SPI = y or m

2.2 Porting the new kernel by activating the TPM

Follow the steps listed below:

1. Upgrade the new Linux kernel (version ≥ 4.14).
2. Check the tutorial available in the *documentation/linux/kernel/building* page at https://www.raspberry.org.
3. Run the local building: in *menu>Preferences>Raspberry PI Configuration*, activate the I2C and SPI interfaces item and disable the underscan system item.
4. Open the terminal with the code below.

```
$sudo -I
#sudo apt-get install bc
#cd /home/pi/Downloads
#git clone -b rpi-4.14.y --depth=1 https://github.com/raspberrypi/linux
```

2.3 Device tree file update for SPI

The DTS (device tree source) configuration (bcm27* files) is done with the following code.

```
#cd /home/pi/Downloads/linux/arch/arm/boot/
#chmod 777 dts
#cd dts
#chmod 777 bcm27*

Replace in all bcm27* files
---------------------------------
spidev0: spidev@0{
compatible = "spidev";
reg=<0>; /* CE0 */
#address-cells = <1>;
#size-cells = <0>;
spi-max-frequency = <500000>;
};

replaced by

st33htpm0: st33htpm@0{
        status="okay";
        compatible = "st,st33htpm-spi";
        reg = <0>;
        #address-cells = <1>;
        #size-cells = <0>;
        spi-max-frequency = <25000000>;

    };
---------------------------------
```

2.4 Device tree file updated for I²C

The I²C TPM driver compatible TCG implementation is not yet available by default in the Linux kernel. Contact your local STMicroelectronics sales office to obtain it.

The DTS configuration (bcm27* files) is done with the following code.

```
#cd /home/pi/Downloads/linux/arch/arm/boot/
#chmod 777 dts
#cd dts
#chmod 777 bcm27*

Replace in all bcm27* files
---------------------------------
&i2c1 {    pinctrl-names = "default";
    pinctrl-0 = <&i2c1_pins>;
    clock-frequency = <100000>;
};
replaced by

&i2c1 {    pinctrl-names = "default";
    pinctrl-0 = <&i2c1_pins>;
    clock-frequency = <400000>;
    st33htpi: st33htpi@0{
        compatible = "st,st33htpm-i2c";
        reg = <0x2E>;
    status="okay";
    };
};
---------------------------------
```

2.5 Configuration specification update

Update the defconfig files in accordance with your Raspberry Pi hardware version (*bcmrpi_defconfig*, *bcm2709_defconfig*, *bcm2711_defconfig* etc.) with the following code.

```
#cd /home/pi/Downloads/linux/arch/arm
#chmod 777 configs
#cd configs
#chmod 777 bcm*

Bcmrpi_defconfig (RPI 1) and bcm2709_defconfig (RPI 2/3) should be updated :
-------------------------------
Config spec we add TCG TPM driver directly in Linux kernel (in Red SPI Only in Purple I2C
only): m means modules driver is not loaded in linux kernel during platform starting.
Modules should be enabled.
-------------------------------
CONFIG_TCG_TPM=y
CONFIG_CRC_CCITT=y
CONFIG_TCG_TIS_CORE=y
CONFIG_TCG_TIS_SPI=m
CONFIG_TCG_TIS_I2C=m
```

2.6 Kernel compilation

The kernel compilation is done with the following code.

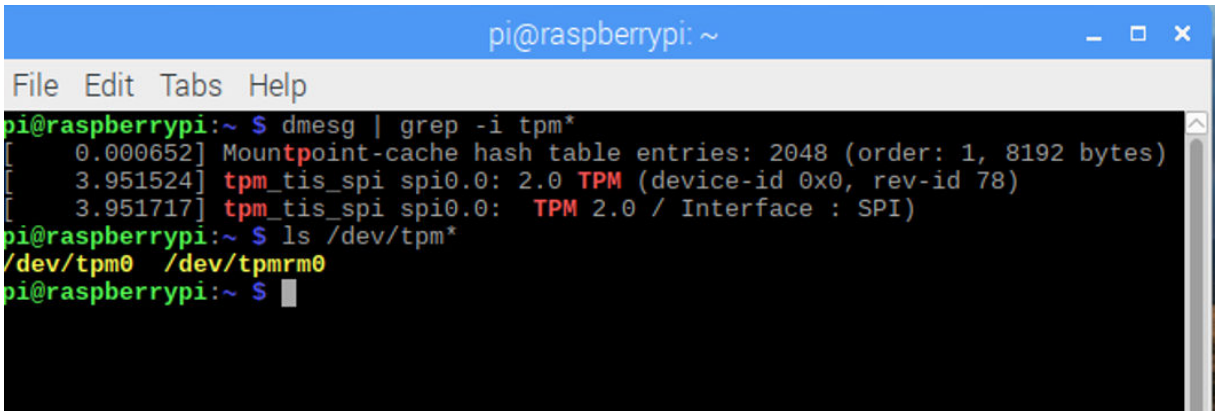
```
---------------------
Configuration to compile RPI 4
---------------------
#cd /home/pi/Downloads/
#cd linux
#KERNEL=kernel7l
# make bcm2711_defconfig
or
---------------------
Configuration to compile RPI 2/3
---------------------
#cd /home/pi/Downloads/
#cd linux
#KERNEL=kernel7
#make bcm2709_defconfig
 or
---------------------
Configuration to compile RPI
---------------------
#cd /home/pi/Downloads/
#cd linux
#KERNEL=kernel
#make bcmrpi_defconfig

---------------------
Start to compile
---------------------
#sudo apt-get install bc
#make -j4 zImage modules dtbs
#sudo make modules_install
#sudo cp arch/arm/boot/dts/*.dtb /boot/
#sudo cp arch/arm/boot/dts/overlays/*.dtb* /boot/overlays/
#sudo cp arch/arm/boot/dts/overlays/README /boot/overlays/
#sudo ./scripts/mkknlimg arch/arm/boot/zImage /boot/$KERNEL.img
```

2.7 TPM driver loading check

When the TPM driver is loaded, `/dev/tpm0` and `/dev/tpmrm0` are present, as shown in the figure below.

Figure 7. Raspbian windows



3 Ordering information

The STPM4RasPI extension board can be ordered using the commercial product names listed in the table below.

Table 1. Ordering information

Commercial product	Description	TPM part numbers
SCT-TPM-RASPIHD0	TPM2.0 (default)/TPM1.2, TCG TPM2.0 spec 1.38, firmware version 0x49.40, SPI interface	ST33TPHF2ESPI
SCT-TPM-RASPIHD1	TPM2.0 only, TCG TPM2.0 spec 1.38, firmware version 0x4A.40, SPI interface	ST33TPHF20SPI
SCT-TPM-RASPIHC2	TPM2.0 (default)/TPM1.2, TCG TPM2.0 spec 1.38, firmware version 0x49.41, I²C interface	ST33TPHF2EI2C
SCT-TPM-RASPIHC3	TPM2.0 only, TCG TPM2.0 spec 1.38, firmware version 0x4A.41, I²C interface	ST33TPHF20I2C
SCT-TPM-RAS2XSPI	TPM2.0 only, TCG TPM2.0 spec 1.38, extended features, firmware version 0x01.102, SPI interface	ST33TPHF2XSPI
SCT-TPM-RASPIHD5	TPM2.0 only, TCG TPM2.0 spec 1.38, extended features, firmware version 0x02.110, I²C interface	ST33TPHF2XI2C

Note: For the description of the soldered products and details on how to order them, refer to the data briefs of the corresponding TPM devices (TPM part numbers defined in the above table).

Revision history

Table 2. Document revision history

Date	Version	Changes
12-Mar-2019	1	Initial release.
11-Oct-2019	2	Updated Section 1.2 Raspberry SPI/I²C connectivity by GPIO. Updated Section 3 Ordering information. Small text changes.
17-Jan-2020	3	Updated Table 1. Ordering information: • Modified the TPM part number corresponding to the SCT-TPM-RASPIHC2 commercial product. • Added the SCT-TPM-RASPIHC3 product.
12-Oct-2020	4	ST33TPM12SPI and ST33TPM12I2C no longer supported. Updated Section 2.1 TPM Linux driver introduction and Section 2.2 Porting the new kernel by activating the TPM. Updated `spi-max-frequency` in Section 2.3 Device tree file update for SPI. Updated Section 2.5 Configuration specification update. Added configuration to compile RPI 4 to Section 2.6 Kernel compilation. Updated Table 1. Ordering information.

Contents

1 **Main features** 2
1.1 Raspberry Pi introduction 2
1.2 Raspberry SPI/I²C connectivity by GPIO 3
1.3 STPM4RasPI setup 4
1.4 TPM power consumption 4
2 **Linux® integration requirements** 5
2.1 TPM Linux driver introduction 5
2.2 Porting the new kernel by activating the TPM 6
2.3 Device tree file update for SPI 6
2.4 Device tree file updated for I²C 7
2.5 Configuration specification update 7
2.6 Kernel compilation 8
2.7 TPM driver loading check 8
3 **Ordering information** 9
Revision history 10
Contents 11
List of figures 12

List of figures

Figure 1. Raspberry Pi 3 Model B . . . 2
Figure 2. Raspberry Pi GPIO . . . 3
Figure 3. STPM4RasPI embedded in the Raspberry Pi board . . . 4
Figure 4. STPM4RasPI embedded in the Raspberry Pi box with touch screen . . . 4
Figure 5. P1 header location . . . 4
Figure 6. TPM directory example in Linux kernel. . . . 5
Figure 7. Raspbian windows . . . 8

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

STMicroelectronics:

SCT-TPM-RAS2XSPI SCT-TPM-RASPIHD5